the step of decrypting a_{new} and b_{new} using the receiver secret key x to get the primary transmitter secret key z is comprised of computing $z = a_{new}/b_{new}^{x}$.

3. (currently amended) The method of claim 1 wherein:

   El Gamal encryption is used for the step of encrypting the data message m [steps].

4. (currently amended) The method of claim 2 wherein:

   El Gamal encryption is used for the step of encrypting the data message m [steps].

5. (original) The method of claim 1 wherein:

   the primary transmitter secret key z is determined from the formula of $z = g^{\gamma}$ modulo p, where γ is a random value chosen from the set [0..q], where q is a value picked using a known encryption method.

6. (currently amended) A method comprising the steps of:

   creating a primary transmitter key z;

   creating a secondary transmitter key z' which is a function of z;

   encrypting a data message m using the secondary transmitter secret key z' to form a quantity E;

   preparing a quadruplet (a_{new}, b_{new}, s_{new}, E) where:

   $a_{new} = z^* y^{c}$ modulo p ;

   $b_{new} = g^{c}$ modulo p;

   $s_{new} = \text{signature}_{c}(a_{new}, b_{new}, E)$;

   where $y = g^{x}$ modulo p, c is a random number, x is a receiver secret key, and the

parameters g, x, and p are picked using a known encryption method;

wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new};

verifying the signature s_{new};

decrypting a_{new} and b_{new} using the receiver secret key x to get the primary transmitter secret key z;

modifying the primary transmitter secret key z to obtain the secondary transmitter secret key z' and using the secondary transmitter secret key z' to decrypt the quantity E and thereby obtaining the message m.

7. (original) The method of claim 6 and wherein:

the primary transmitter key z is provided which is not of the format used for producing the ciphertext E;

the secondary transmitter key z' is computed as a function of z, where the function is an arbitrary function.

8. (currently amended) A method comprising the steps of:

creating a primary transmitter key z;

creating a secondary transmitter key z' which is a function of z;

providing a plurality of portion keys which are derived from the secondary transmitter key z';

encrypting a data message m using the plurality of portion keys to form a quantity E;

preparing a quadruplet (a_{new}, b_{new}, s_{new}, E) where:

$a_{new} = z^* y^c$ modulo p ;
$b_{new} = g^c$ modulo p;
s_{new} = signature $_c(a_{new}, b_{new}, E)$;

where $y = g^x$ modulo p, c is a random number, x is a receiver secret key, and the parameters g, x, and p are picked using a known encryption method;

wherein s_{new} is a signature which is determined by using the same random number c that was used to determine a_{new} and b_{new};

verifying the signature s_{new};

decrypting a_{new} and b_{new} using the receiver secret key x to get the primary transmitter secret key z;

modifying the primary transmitter secret key z to obtain the secondary transmitter secret key z' and using the secondary transmitter secret key z' to determine the plurality of portion keys and using the plurality of portion keys to decrypt the quantity E and thereby obtaining the message m.

9. (new) The method of claim 1 wherein

the signature s_{new} is determined by using a Schnorr signature method.

10. (new) The method of claim 1 wherein

the signature s_{new} is determined using a Digital Signature Standard.

11. (new) An apparatus comprising

a processor;

wherein the processor

encrypts a data message m using a primary transmitter secret key z to form a quantity E; and

prepares a quadruplet (a_{new}, b_{new}, s_{new}, E) where:

$a_{new} = z^* y^c$ modulo p ;

$b_{new} = g^c$ modulo p;

s_{new} = signature $_c(a_{new}, b_{new}, E)$;

where $y = g^x$ modulo p, c is a random number, x is a receiver secret key, and the parameters g, x, and p are picked using a known encryption method; and

wherein s_{new} is a signature, and wherein the processor determines s_{new} by using the same random number c that was used to determine a_{new} and b_{new}.

12. (new) The apparatus of claim 11 wherein the processor uses El Gamal encryption to encrypt the data message m.

13. (new) The apparatus of claim 11 wherein the processor uses a Schnorr signature method to determine s_{new}.

14. (new) The apparatus of claim 11 wherein the processor uses a Digital Signature Standard to determine s_{new}.